IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEBRASKA

PRISM TECHNOLOGIES, LLC,

Plaintiff,

v.

ADOBE SYSTEMS INCORPORATED; AUTODESK, INC.; MCAFEE, INC.; NATIONAL INSTRUMENTS CORPORATION; NUANCE COMMUNICATIONS, INC.; QUARK, INC.; THE SAGE GROUP PLC; SAGE SOFTWARE, INC.; SYMANTEC CORPORATION; THE MATHWORKS, INC.; and TREND MICRO INCORPORATED,

Defendants.

Case No. 8:10-CV-00220-LES-TDT

PLAINTIFF PRISM TECHNOLOGIES, LLC'S OPENING CLAIM CONSTRUCTION BRIEF

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

CASES

I. INTRODUCTION

Plaintiff Prism Technologies, LLC ("Prism") respectfully submits this brief regarding the proper construction of various disputed terms in U.S. Patent No. 7,290,288 ("the '288 patent"), the patent at issue in this litigation. At Defendants' request, this Court has already construed two disputed claim terms – "hardware key" and "access key" – based on Defendants' assertion that the construction of those terms could be case-dispositive on the issue of infringement. (Dkt. No. 188). But the Court's construction of "hardware key" and "access key" was not case-dispositive as Defendants had hoped, thereby necessitating the further construction of the remaining disputed terms in the '288 patent claims.

Importantly, in construing "hardware key" and "access key," this Court relied in part on a Delaware district court's claim construction order in a previous case, *Prism Technologies, LLC v. VeriSign, Inc. et al.*, Case No. 05-214-JJF (D. Del.) ("the *VeriSign* case"). In that case, the Delaware court construed claim terms in the related U.S. Patent No. 6,516,416 ("the '416 patent"), of which the '288 patent is a continuation-in-part. The Delaware claim construction order was ultimately affirmed on appeal. The inventors of the '288 patent further disclosed the Delaware claim construction order to the patent examiner during prosecution of the '288 patent, thereby making the Delaware claim construction a part of the '288 patent's file history. Taking into account these facts, this Court noted that "[p]rior constructions of identical claim terms in related patents are highly relevant to construing claim terms," and ultimately adopted the same construction of "hardware key" as the Delaware district court, and construed "access key" to mean the same thing as "hardware key." (Dkt. No. 188 at 11, 14).

Many of the remaining disputed claim terms of the ’288 patent are identical or highly similar to claim terms of the ’416 patent that were previously construed by the Delaware court. Applying the same reasoning, these remaining terms should be construed in accordance with the Delaware court’s constructions in the *VeriSign* case, consistent with this Court’s approach in construing “hardware key” and “access key.” As to the terms presented in this brief, the Delaware court’s constructions are well-reasoned and supported by the language of the ’288 claims, the specification, and the prosecution history, and are furthermore consistent with extrinsic evidence from dictionaries and testimony from Prism’s expert witness. In addition, the Delaware court’s constructions are also part of the ’288 file history, and therefore serve to inform the public as to the scope of the ‘288 patent claims. Those constructions should therefore be adopted in this case.

And although Defendants previously advocated following the Delaware court’s claim construction order, they now ignore that order and propose overly-narrow constructions of the patent claims that deviate completely from the ’288 claim language, specification, prosecution history, and the Delaware court’s claim construction. Defendants’ proposals likewise violate the principle that the patent specification cannot be used to import limitations into the claims. Defendants’ proposed constructions are therefore untenable. Only Prism’s proposed constructions, which comport with the claims language, specification, prosecution history, and the Delaware court’s constructions, are consistent with the intrinsic and extrinsic evidence. Indeed, as even Defendants previously argued, “[t]he Court should adopt the Delaware court’s construction as-is because . . . it stays true to the claim language and most naturally aligns with the patent’s description of the invention.” (Defendants’ Opening Claim Construction Brief

Regarding "Hardware Key" and "Access Key," Dkt. No. 172 at 2). Thus, Prism respectfully requests that the Court adopt Prism's proposed claim constructions as set forth below.

I. BACKGROUND

A. The '288 Patent

The United States Patent & Trademark Office ("PTO") issued the '288 patent on October 30, 2007. (Ex. B, '288 patent).[1] The '288 patent contains 187 claims in total. Prism presently asserts that Defendants infringe the following claims of the '288 patent: 1-3, 13, 21-23, 27, 31-36, 46, 51, 54, 56, 62-64, 81, 82, 85, 87, 88-93, 103, 110, 111, 117, 131, 134, 135, 143, 145, 146, 150, 165, 168, 169, 178, 180, and 185-187.[2]

The '288 patent covers an innovative way of controlling access to computer resources requested by a client computer device over a computer network. (Ex. B at 1:52-54). More specifically, the systems and methods disclosed by the '288 patent control access to computer resources using a server with an associated database that stores information that can be used to authenticate client and server devices and determine which devices are authorized to access computer resources in the network. To ensure that the client computer device is properly authorized to access the computer resources, the client computer device has an associated hardware key that contains a digital identification used to authenticate the device to the system. Figure 3 of the patent sets forth a basic overview of one embodiment of the invention:

---

[1] References herein to "Ex. [X]" refer to an exhibit to the Index of Evidence filed concurrently with this brief.

[2] Not all of these claims are asserted against every Defendant, however.

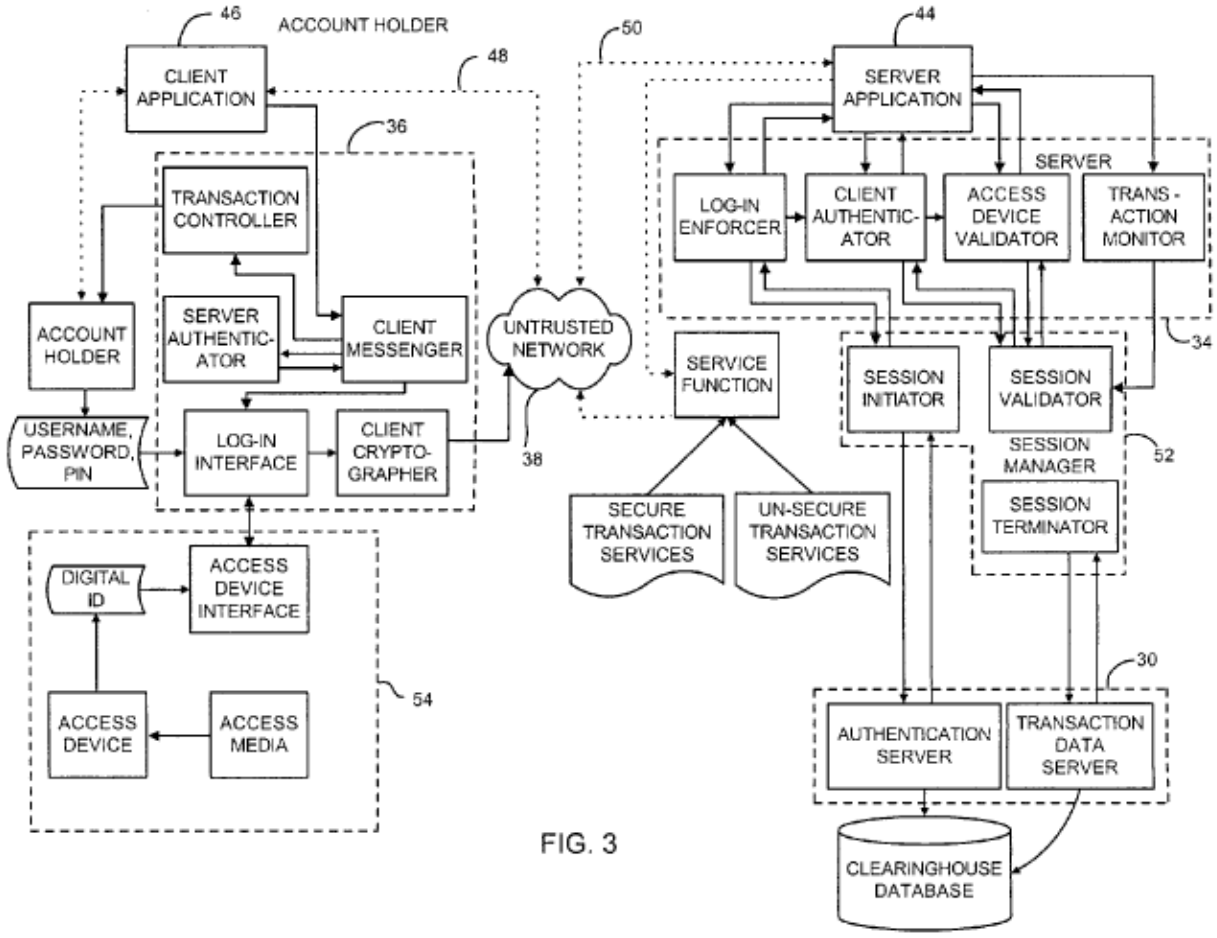

FIG. 3

(Ex. B at Fig. 3).

As described in the specification, Figure 3 shows an "account holder computer" (block 36) with an associated "hardware key" (block 54) that communicates with a "secure transaction server" (block 34) over a network. (Ex. B at 5:5-7, 6:26-35). The "secure transaction server" in turn communicates with a "transaction clearinghouse" (block 30) through a "session manager" (block 52). (*Id.* at 6:31-35).

In operation, when the client computer device sends a request to access the protected resources, it forwards a digital identification derived from the hardware key as well as, in some cases, additional identifying information to the secure transaction server so that it can be authenticated by the system. (*Id.* at 5:23-45, 6:7-18). The secure transaction server in turn sends the information from the client computer device to the transaction clearinghouse. (*Id.* at 6:15-18).

The transaction clearinghouse is associated with a database that stores identifying information for client and server computers in the system, as well as authorization data associated with the protected computer resources. (*Id.* at 4:14-39; 6:51-56; *see also id.* at 1:49 – 2:13). Using this information, the transaction clearinghouse can determine whether the client computer device is authentic and authorized to access the protected computer resources. (*Id.* at 6:47 – 7:16). The transaction clearinghouse also has the ability to authenticate servers in the system to ensure that data is being sent to and from the proper locations. (*Id.* at 7:6-16). These inventive concepts are embodied within various claims of the ’288 patent.[3]

For purposes of claim construction, it is useful to consider the asserted independent claims as falling into two general categories: (1) the “server computer/clearinghouse” claims (claims 1, 31, 62, and 87), and (2) the “access server/authentication server” claims (claims 117,

[3] Importantly, the ’288 specification describes one-factor, two-factor, and three-factor authentication systems and methods. (*See, e.g.*, Ex. B at 16:64-17:1). “Factor” in this context means generally a piece of data used for authentication. Thus, a “two-factor” authentication system would require a user or device to present two different pieces of data to authenticate the user or device. Some of the asserted ’288 claims, such as claim 1, require the use of only one piece of data for authentication.

150, and 185-187). Claim 1, which is representative of the "server computer/clearinghouse" claims, recites:

> 1. A system for protecting resources of at least one server computer, said at least one server computer providing said protected resources to at least one client computer device via an untrusted network, without necessarily protecting other computer resources provided by said at least one server computer and by other server computers to other client computer devices, comprising:
>
> at least one clearinghouse for storing (i) identity data of said at least one server computer and (ii) identity data of each of said at least one client computer device and (iii) authorization data associated with said protected resources;
>
> server software installed on said at least one server computer that forwards the identity data of said at least one server computer and the identity data of each of said at least one client computer device to said at least one clearinghouse;
>
> client software installed on each of said at least one client computer device that forwards its identity data to said at least one server computer;
>
> at least one hardware key associated with said at least one client computer device, said at least one hardware key generating a digital identification, the identity data of said at least one client computer device comprising said digital identification;
>
> said server software installed on said at least one server computer selectively requiring said at least one client computer device to forward said digital identification to said at least one server computer;
>
> said at least one clearinghouse authenticating the identity of said at least one client computer device responsive to a request for said protected resources of said at least one server computer by said at least one client computer device;
>
> said at least one clearinghouse authenticating the identity of said at least one server computer responsive to said at least one client computer device making the request for said protected resources of said at least one server computer;
>
> said at least one clearinghouse authorizing said at least one client computer device to receive said requested protected resources, based on said stored authorization data;
>
> and, said at least one clearinghouse controlling access to said requested protected resources of said at least one server computer responsive to successful

> authentication of said at least one server computer and of said at least one client computer device making the request and responsive to successful authorization of said at least one client computer device.

(Ex. B at 34:54 – 35:36).

Claim 117 of the '288 patent, which is representative of the "access server/authentication server" claims, recites:

> 117. A system for controlling access to protected computer resources provided via an Internet Protocol network, the system comprising:
>
> at least one authentication server having an associated database to store (i) identity data of at least one access server, (ii) a digital identification associated with at least one client computer device requesting access to said protected computer resources, and (iii) data associated with said protected computer resources;
>
> said at least one client computer device having an associated access key, said digital identification being derived from said access key;
>
> said at least one client computer device adapted to forward said digital identification to said at least one access server;
>
> said at least one access server adapted to forward, to said at least one authentication server, said identity data and said digital identification received from said at least one client computer device;
>
> said at least one authentication server adapted to authenticate said identity data and said digital identification responsive to a request for said protected computer resources by said at least once client computer device;
>
> said at least one authentication server adapted to authorize said at least one client computer device to receive at least a portion of said requested protected computer resources, based on said stored data associated with said requested protected computer resources;
>
> and said at least one authentication server adapted to permit access to said at least said portion of said requested protected computer resources upon successfully authenticating said identity data and said digital identification and upon successfully authorizing said at least once client computer device.

(Ex. B at 45:1-36).[4]

For the Court's convenience, a complete recitation of the asserted independent claims of the '288 patent is attached hereto as Exhibit C.

B. The Delaware Claim Construction Order

The '288 patent is a continuation-in-part of another patent, U.S. Patent No. 6,516,416 ("the '416 patent") (Ex. D). The '416 patent was asserted by Prism in a previous litigation, *Prism Techs. LLC v. VeriSign, Inc.*, No. 05-214-JJF, in the District of Delaware ("the *VeriSign* case"). In that case, the Delaware court construed various claim terms in the '416 patent, issuing a thoroughly-reasoned Memorandum Opinion explaining the basis for its constructions as well as a more concise Order summarizing its constructions. (Exs. E and F). On appeal, the Federal Circuit affirmed those constructions without comment. *Prism Techs. LLC v. VeriSign, Inc.*, 263 F. App'x 878 (Fed. Cir. 2008).

The Delaware court issued its claim construction in the *VeriSign* case while the application for the '288 patent was still pending before the PTO. The inventors of the '288 patent therefore disclosed the Delaware claim construction order to the patent examiner so that he could take the Delaware court's constructions into account when considering whether to allow the '288 patent claims. As already established by this Court, the disclosure of the Delaware claim construction order during the prosecution of the '288 patent makes the Delaware claim construction an official part of the '288 patent's prosecution history. (Dkt. No. 188 at 11).

[4] While claims 1 and 117 are product claims, Prism is also asserting method claims against Defendants.

As discussed in more detail below, a number of the disputed claim terms in this action are identical or nearly identical to claim terms that were previously construed by the Delaware court.

C. This Court's Prior Claim Construction Order

On April 11, 2011, this Court held a hearing regarding the proper construction of only two claim terms in the '288 patent: "hardware key" and "access key." (Dkt. No. 185). Defendants requested that the Court stay discovery and issue a construction of these two terms before the case was allowed to proceed, because Defendants claimed that the construction of the terms would be dispositive of the issue of infringement. (*See* Dkt. No. 155 at 9-10).[5]

On June 8, 2011, the Court issued its claim construction for the terms "hardware key" and "access key." (Dkt. No. 188). In its order, the Court adopted the Delaware court's construction of "hardware key" verbatim.[6] (*Id.* at 14). In explaining its reasons for adopting the Delaware construction of "hardware key," the Court noted as highly relevant the fact that Prism cited the Delaware claim construction order to the PTO during prosecution of the '288 patent, thereby making the Delaware order a part of the '288 prosecution history. (*Id.* at 11-12). The Court also relied on the case law holding that "[p]rior constructions of identical claim terms in related patents are highly relevant to construing claim terms." (*Id.* at 11).

[5] Prism opposed the piecemeal claim construction procedure and the stay.

[6] The parties agreed that "access key" should have the same construction as "hardware key," and thus the Court applied its definition of "hardware key" to "access key" as well.

II. ARGUMENT

A. Applicable Law

"[T]he claims of a patent define the invention to which the patentee is entitled the right to exclude." *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005) (en banc) (quoting *Innova/Pure Water, Inc. v. Safari Water Filtration Sys., Inc.*, 381 F.3d 1111, 1115 (Fed. Cir. 2004)). In construing terms, courts must give each term its "ordinary and customary meaning," which is "the meaning that the term would have to a person of ordinary skill in the art in question at the time of the invention." *Id.* at 1313. Where the meaning of a term is not immediately apparent, courts must look at "those sources available to the public that show what a person of skill in the art would have understood disputed claim language to mean," including "the words of the claims themselves, the remainder of the specification, the prosecution history, and extrinsic evidence concerning relevant scientific principles, the meaning of technical terms, and the state of the art." *Id.* at 1314 (quoting *Innova*, 381 F.3d at 1116).

"[I]n interpreting an asserted claim, the court should look first to the intrinsic evidence of record, *i.e.*, the patent itself, including the claims, the specification and, if in evidence, the prosecution history." *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1582 (Fed. Cir. 1996). "[T]he claims themselves provide substantial guidance as to the meaning of particular claim terms." *Phillips*, 415 F.3d at 1314. For example, "the context in which a term is used in the asserted claim can be highly instructive," and "[o]ther claims of the patent in question, both asserted and unasserted, can also be valuable sources of enlightenment as to the meaning of a claim term." *Id.* In addition, under the doctrine of claim differentiation, "the presence of a dependent claim that adds a particular limitation gives rise to a presumption that the limitation in

question is not present in the independent claim." *Id.* at 1315. This presumption is "especially strong when the limitation in dispute is the only meaningful difference between an independent and dependent claim, and one party is urging that the limitation in the dependent claim should be read into the independent claim." *SunRace Roots Enter. Co., Ltd. v. SRAM Corp.*, 336 F.3d 1298, 1303 (Fed. Cir. 2003).

"[T]he specification 'is always highly relevant to the claim construction analysis. Usually, it is dispositive; it is the single best guide to the meaning of a disputed term.'" *Phillips*, 415 F.3d at 1315 (citation omitted). "The longstanding difficulty is the contrasting nature of the axioms that (a) a claim must be read in view of the specification and (b) a court may not read a limitation into a claim from the specification." *Innova*, 381 F.3d at 1117. The Federal Circuit has explained that it is only in very limited circumstances, such as when the patentee provides a special definition to a claim term or intentionally disclaims subject matter, where the specification may limit the meaning of the claim language. *See Phillips*, 415 F.3d at 1316. Furthermore, the Federal Circuit has admonished that "although the specification often describes very specific embodiments of the invention, we have repeatedly warned against confining the claims to those embodiments." *Id.* at 1323.

The prosecution history is also relevant to construing the claims, as it "provides evidence of how the PTO and the inventor understood the patent." *Id.* at 1317. The prosecution history "consists of the complete record of the proceedings before the PTO and includes the prior art cited during the examination of the patent." *Id.*

Extrinsic evidence "consists of all evidence external to the patent and prosecution history, including expert and inventor testimony, dictionaries, and learned treatises." *Phillips*, 415 F.3d

at 1317 (internal citations and quotations omitted). Extrinsic evidence is generally viewed as less reliable than intrinsic evidence, but nevertheless "can help educate the court regarding the field of the invention and can help the court determine what a person of ordinary skill in the art would understand claim terms to mean." *Id.* at 1319.

B. Agreed-Upon Constructions

The parties have agreed to the constructions of the following two terms appearing in independent claims 1, 31, 62, and 87 of the '288 patent:[7]

Claim Term	Proposed Construction
"**an untrusted network**" (independent claims 1, 31, 62, 87)	a public network with no controlling organization, with the path to access the network being undefined and the user being anonymous
"**server computer**" (independent claims 1, 31, 62, 87)	a computer that makes available information or other resources

C. "protected resources" and "protected computer resources"

The parties propose the following constructions for the terms "protected resources" and "protected computer resources" in the asserted claims of the '288 patent:

Claim Term	Prism's Proposed Construction	Defendants' Proposed Construction
"**protected resources**" (independent claims 1, 31, 62, 87)	computer services, applications, or content that can be accessed by (either directly or indirectly) said server computer	computer services, applications, or content that can be accessed (either directly or indirectly) by said server computer, but are not stored on the client computer device

[7] The parties submitted to the Court their proposed claim constructions in a Joint Claim Construction Statement filed on September 19, 2011. (Dkt. No. 276).

"**protected computer resources**" (independent claims 117, 150, 185-187)	computer services, applications, or content that can be accessed by (either directly or indirectly) said access server	computer services, applications, or content that can be accessed (either directly or indirectly) by said server computer, but are not stored on the client computer device

Prism's proposed construction of "protected resources" and "protected computer resources" is based on the Delaware court's construction of a similar phrase in the '416 patent claims, "selected computer resources of at least a [or said] first server computer." The Delaware court construed that phrase as "computer services, applications, or content that can be accessed by (either directly or indirectly) said first server computer." (Ex. F at 2). Prism's proposed construction of "protected resources" in claims 1, 31, 62, and 87 tracks the Delaware construction, with the only change being to delete the term "first" before "server computer" because claims 1, 31, 62, and 87 refer to a "server computer" rather than a "first server computer." Similarly, Prism's proposed construction of "protected computer resources" closely tracks the Delaware construction, but changes "said first server computer" to "said access server" because the '288 patent claims in which the term "protected computer resources" appears (claims 117, 150, and 185-187) refer to an "access server" rather than a "first server computer."

Defendants generally agree with the language in Prism's proposed construction regarding "computer services, applications, or content that can be accessed by (either directly or indirectly)" a server. Defendants' proposed constructions, however, improperly add the requirement that the computer services, applications, or content "are not stored on the client computer device." This additional language is not found in the claims and is not required by the patent's written description. There is nothing in the '288 patent claims, specification, or prosecution history that requires the "protected resources" or "protected computer resources" to

be stored in any particular location. Rather, the patent leaves open the possibility that these resources could be located anywhere within the network.

Importantly, this issue was previously raised before the Delaware court with respect to the '416 patent, and the Delaware court found that the protected resources do not need to be stored at any particular location.[8] The Delaware claim construction order, and by extension the '288 prosecution history as well, therefore directly contradicts Defendants' proposed construction.

Specifically, in the *VeriSign* case the defendants proposed that the claim language "selected computer resources of at least a [or said] first server computer" should be construed as "the restricted resources requested by the subscriber client computer that are located on the first server computer." (Ex. G at 20). The defendants argued that the claim language referring to computer resources "of" a first server computer meant that the "computer resources" needed to be ***on*** the first server computer. (Ex. H at 65:16-66:23). The Delaware court rejected the defendants' proposed construction, reasoning:

> [T]he system disclosed in the specification and corresponding figures does not require the first server computer to store the resources it communicates to subscribers. Rather, it allows the server to act as a gatekeeper, accessing selected computer resources protected by the invention either itself or through a "Service Function" block, and communicating those resources to subscribers.

(Ex. E at 13-14). The Delaware court therefore refused to read into the claim limitation "selected computer resources of at least a [or said] first server computer" in the '416 claims a requirement

[8] As this Court has previously noted, the Delaware court's construction of terms in the '416 patent is highly relevant to claim construction for the '288 patent. *See* June 1, 2011 Memorandum and Order (Dkt. No. 188), at 11-12.

that the "selected computer resources" must be located at any particular location. This Court should similarly reject Defendants' attempt to read into the '288 claims a limitation regarding where the protected resources of the system can or cannot be stored.

Finally, Defendants' proposed construction of "selected computer resources" is also flawed because it refers to computer services, applications, or content that can be accessed "by said server computer." Claims 117, 150, and 185-187 in which the phrase "selected computer resources" appears, however, do not contain the term "server computer." Thus, Defendants' proposed language "by said server computer" would not make any sense in claims 117, 150, and 185-187.

D. "digital identification"

The parties propose the following constructions for the term "digital identification" in the asserted claims of the '288 patent:

Claim Term	Prism's Proposed Construction	Defendants' Proposed Construction
"**digital identification**" (independent claims 1, 31, 62, 87, 117, 150, 185-187)	digital data whose value is known in advance or calculated at the moment	digital data that uniquely identifies the account holder to whom the hardware key (or access key) is issued

In the '288 claims, the "digital identification" is information associated with either a "hardware key" or "access key" and used in the process of authenticating and authorizing access to protected resources. For example, claim 1 recites "at least one hardware key associated with said at least one client computer device, said at least one hardware key generating a digital identification." Furthermore, this Court has construed "hardware key" and "access key" to mean "an external hardware device or object from which the predetermined digital identification can

be read." (Dkt. No. 188 at 15). Thus, while the claims and the Court's previous claim construction order require a particular relationship between the "digital identification" and the "hardware key/access key," the Court has yet to address the separate issue of what "digital identification" means.

Prism's proposed construction of "digital identification" follows the Delaware court's construction of the term "predetermined digital identification" in *VeriSign*, whereas Defendants propose an entirely new construction of "digital identification" that departs significantly from the Delaware construction.

In *VeriSign*, the court construed the term "predetermined digital identification" in the '416 patent claims as "digital data whose value is known in advance or calculated at the moment." (Ex. F at 2). That same construction should apply to the term "digital identification" in the '288 patent. As this Court noted in its previous Memorandum and Order construing the terms "hardware key" and "access key," "[p]rior constructions of identical claim terms in related patents are highly relevant to construing claim terms." (Dkt. No. 188 at 11). *See also Omega Eng'g, Inc. v. Raytek Corp.*, 334 F.3d 1314, 1334 (Fed. Cir. 2003) ("we presume, unless otherwise compelled, that the same claim term in the same patent or related patents carries the same construed meaning"). Moreover, by construing "hardware key" and "access key" as "an external hardware device or object from which ***the predetermined digital identification*** can be read," this Court has already determined that the "digital identification" in the '288 claims is the same as the "predetermined digital identification" in the '416 claims. This Court further noted that, since the Delaware court's claim construction was cited to the examiner during prosecution

of the ‘288, it is a part of the ‘288 prosecution history, and thus particularly relevant to the construction of the ‘288 claims. (Dkt. No. 188 at 11-12).

As the Delaware court’s construction recognizes, the claims use the term “digital identification” broadly to mean any piece of data that is either known in advance or calculated at the moment so that it can be used to authenticate a user or a device over a network. One of ordinary skill in the art reading the ’288 prosecution history would understand that this construction by the Delaware court of “digital identification” applies equally to the usage of that term in the ’288 patent claims. (*See* Ex. I, Declaration of David Klausner in Support of Prism’s Opening Claim Construction Brief, at ¶¶ 12-16).

Rather than staying true to the Delaware court’s construction of “predetermined digital identification,” Defendants propose an entirely new construction of “digital identification,” namely “digital data that uniquely identifies the account holder to whom the hardware key (or access key) is issued.” Defendants’ construction is unduly restrictive in that it requires the digital identification to specifically identify one individual, “the account holder to whom the hardware key (or access key) is issued.” There is nothing in the language of the claims that requires the digital identification to be associated with an “account holder.” Indeed, Defendants’ proposed construction must be rejected because it would directly contradict the plain language of asserted claims 117, 150, 186, and 187. Each of these claims contains the limitation “a digital identification ***associated with at least one client computer device***.” (Ex. B at 45:6-7, 47:27-28, 50:38-39, 51:5-6) (emphasis added). In other words, these claims recite a digital identification that can be associated with ***multiple*** client computer ***devices***, and thus would not “uniquely identif[y] the account holder to whom the hardware key (or access key) is issued.” Rather, for

these claims a single digital identification is used to identify a set of devices that can be authorized to access the protected resources, rather than a single individual. (*See* Ex. I, ¶ 17).

Additionally, the specification describes embodiments of the "hardware key" that would not necessarily "uniquely identify" a specific individual. For example, the specification describes using magnetic cards as hardware keys. (Ex. B at 20:29-47). The specification explains:

> A magnetic card is a plastic card with a strip of magnetic recording tape adhered to the back of the card. The magnetic recording strip has three tracks that can be used for storing and retrieving data. In the context of the preferred embodiment, the magnetic card **500** is the preferred access media containing a digital ID.

(*Id.* at 20:34-39). Magnetic cards can, but do not always, specifically identify a specific individual. For example, a company could choose to issue the same magnetic card to multiple individuals who share the same level of security access to a particular resource. In such instances, the magnetic card would not need to contain specific information tying it to only one person or "account holder." Such a card, however, would still restrict access to protected resources.[9] (*See* Ex. I, ¶ 17).

Defendants' proposed construction must therefore be rejected because it would read out of the claims at least one of the "hardware key" embodiments in the patent. *See SanDisk Corp. v. Memorex Prods., Inc.*, 415 F.3d 1278, 1285 (Fed. Cir. 2005) ("A claim construction that

---

[9] For example, the patent specification notes that "[m]agnetic card technology is widely utilized in . . . transportation, and access control." (Ex. B at 20:44-47). At the time of the invention of the '288 patent in the late 1990s and continuing to this day, public transportation systems such as San Francisco's BART subway system have utilized magnetic cards to control riders' access to the system. Some of the types of magnetic cards that riders can purchase do not uniquely identify the individual who purchased the card, but instead can be transferred between individuals. (*See* Ex. J).

excludes a preferred embodiment, moreover, 'is rarely, if ever, correct.'") (quoting *Vitronics*, 90 F.3d at 1583).

Importantly, the issue of whether the term "digital identification" includes a requirement of "uniquely identifying" a specific user was previously considered and rejected by the Delaware court. There, the defendants proposed a construction that included a "uniqueness" limitation, and Prism proposed (and the Delaware court adopted) the same construction Prism proposes now – a construction without a "uniqueness" limitation. (*See* Ex. G at 20). Specifically, the defendants in *VeriSign* argued that "predetermined digital identification" should be construed as "a data string that is preassigned and ***unique*** to the hardware key and that cannot be shared with other users." (*Id.*) (emphasis added). During the claim construction hearing before the Delaware court, counsel for defendants Computer Associates and Netegrity argued at length as to why "predetermined digital identification" should be construed to require a data string that is "unique" to a single person and a single hardware/access key, stating:

> [T]he specification makes absolutely clear that the hardware key contains a ***unique*** digital identification that is microcoded into it. In Column 14, when you apply for a subscription, you get a hardware key with a ***unique*** digital identification microcoded into the access key. . . .
>
> The defendants' proposed construction [of "predetermined digital identification"], a data string that is pre-assigned and ***unique*** to the hardware key ***and that cannot be shared with other users*** is based on the specification and is consistent with how it is used in the invention. . . .
>
> There really should be no discussion here, no dispute, that predetermined digital identification means pre-assigned. And there really should be no dispute that it has to be a – has to be a ***unique*** digital I.D.
>
> This is – the specification is replete with statements, hardware key with a ***unique*** digital I.D., contains a ***unique*** – the access key contains a ***unique*** digital identification that is microcoded into it. In order to serve as an identifier, it has to

> be a ***unique*** digital identification, and closely related to that, ***it cannot be shared with others***.

(Ex. H at 89:4-91:19) (emphasis added).

The Delaware court therefore heard extensive argument as to why "predetermined digital identification" should be construed as something that is "unique" and "preassigned." Nevertheless, the court rejected that construction, and instead adopted the construction "digital data whose value is known in advance or calculated at the moment." The court reasoned:

> Plaintiff contends that the "predetermined digital identification" can be known in advance or calculated at the moment it is verified. Conversely, Defendants argue that the "predetermined digital identification" cannot be calculated at the moment because it must be a unique preassigned data string that cannot be shared with others.
>
> Defendants base their contention on language in the specification calling for the "predetermined digital identification" to be microcoded onto a subscriber's hardware key. . . . However, the language in Claims 1 and 24 does not require that the hardware key be microcoded with a "predetermined digital identification." Rather, Claim 1 refers to "at least one hardware key being adapted to generate a predetermined digital identification," with no specific limitation on when that information is generated. . . . Moreover, Defendants' proposed construction would invalidate dependant claims 6 and 31, which each state that the first server computer can change the predetermined digital identification. . . .
>
> In light of these considerations, and guided by the claim and specification language, the Court declines to import the specification limitation of microcoding into the claim language as Defendants' propose. Instead, the Court construes the term "predetermined digital identification" to mean "digital data whose value is known in advance or calculated at the moment."

(Ex. E at 21-22). The Delaware court's rationale for rejecting the defendants' "preassigned and unique" argument and adopting Prism's construction of "predetermined digital identification" instead was sound, and there is no reason to diverge from it here. *See* Memorandum and Order, Dkt. No. 188 at 14 ("given that the '288 patent and '416 patent are related patents sharing identical terms, the Delaware district court's use of 'read' in its construction of 'hardware key'

lends substantial support to making an identical construction in this case."); *NTP, Inc. v. Research in Motion, Ltd.*, 418 F.3d 1282, 1293 (Fed. Cir. 2005) ("Because NTP's patents all derive from the same parent application and share many common terms, we must interpret the claims consistently across all asserted patents.").

Defendants will likely try to focus the Court's attention to one passage of the '288 patent specification that states:

> The major function of the hardware token access device 450 is to uniquely identify a [sic] account holder that desires to access the transaction services and computer resources of an untrusted network, such as the Internet.

(Ex. B at 19:38-42). Defendants argue that this portion of the specification supports its construction of "digital identification" as "digital data that uniquely identifies the account holder to whom the hardware key (or access key) is issued." But this sentence merely relates to ***one of many*** embodiments of the "hardware key" disclosed in the specification – namely, a physical "token" device depicted in Figure 21 of the patent. (*See* Ex. B at 19:30-33; Fig. 21). And it is a well-established principle of claim construction that the claims cannot be confined to the embodiments described in the specification. *See Phillips*, 415 F.3d at 1323.

For example, the Federal Circuit's decision in *Arlington Industries, Inc. v. Bridgeport Fittings, Inc.*, 345 F.3d 1318 (Fed. Cir. 2003), is particularly instructive. *Arlington* involved a patent relating to electrical box extenders for use in the construction industry. The claims at issue recited a box with wings "capable of flexing" about a base so that the body of the box could fit in a variety of locations. During claim construction, the defendant argued that the claim term "capable of flexing" should be limited to one type of flexing – cantilever flexing – because the only teaching of "flexing" in the patent's written description was one passage in the

specification referring to "flexing of the wings" as "cantilever bending." *Id.* at 1327. The district court rejected this narrow construction of "capable of flexing," and instead construed this phrase more broadly as "a generalized combination of cantilever bending and bowing about the general area of the base or base end." *Id.* at 1325. On appeal, the Federal Circuit affirmed the district court's construction, noting:

> Bridgeport equates this "cantilever bending" with "cantilever flexing," and essentially invites us to import a limitation from the preferred embodiments to restrict the meaning of a claim term. We have consistently warned against this approach to claim construction, which is seldom justified. . . . There is no indication in the written description of the '674 patent, for example, that Gretz "acted as his own lexicographer and clearly set forth a definition of the disputed claim term." . . . Nor do we discern therein any express disclaimer of a particular meaning of "flexing." . . . We accordingly decline Bridgeport's invitation to restrict the meaning of the claim term based on the description of the preferred embodiments.

Id. at 1327. Similarly, Defendants ask the Court to restrict "digital identification" to mean only those digital identifications that can uniquely identify account holders to which a hardware key has been issued, an embodiment that is certainly described in the specification, but is by no means the only way in which the invention can be practiced. Under the law that patent claims cannot be confined to the embodiments described in the specification, such a construction must be rejected.

E. "identity data"

The parties propose the following constructions relating to the term "identity data," which appears in various of the asserted claims of the '288 patent:

Claim Term	Prism's Proposed Construction	Defendants' Proposed Construction
"identity data" (independent claims 1, 31, 62, 87, 117, 150, 185)	data sufficient for the system to determine whether a person, organization, and/or computer is authentic and/or is entitled to access protected resources	Defendants believe that the Court should not construe the term "identity data" in isolation but rather in the context of the relevant claim language, as set forth [below].
"**identity data of [the] client computer device**" (independent claims 1, 31, 62, 87)	No separate construction necessary in light of Prism's proposed construction of "identity data."	data, including the digital identification as well as some additional data (e.g., a username and/or a password), that uniquely identifies the account holder using the client computer device

The Delaware court construed "identity data" as that term appears in the claims of the'416 patent to mean "data sufficient for the patented system to determine whether a person, organization, and/or computer is authentic and/or is entitled to a[cc]ess said selected computer resources." (Ex. E at 24). Prism proposes that the Delaware construction of "identity data" should be adopted for the asserted claims of the '288 patent as well, with only slight modification so that the construction comports with the language of the '288 claims (which refer to "protected resources" rather than "selected computer resources"). *See Omega Eng'g*, 334 F.3d at 1334 ("we presume, unless otherwise compelled, that the same claim term in the same patent or related patents carries the same construed meaning").

Defendants, on the other hand, reject the Delaware construction entirely. Instead, Defendants want to construe the phrase "identity data of [the] client computer device" as "data, including the digital identification as well as some additional data (e.g., a username and/or a password), that uniquely identifies the account holder using the client computer device." Defendants' proposal is untenable for several reasons.

First, the term "identity data" in the '288 claims is not used solely in connection with the term "client computer device." Rather, as shown in the chart below, various '288 claims also refer to "identity data" of a "server computer" or "access server":

Claim 1	"at least one clearinghouse for storing (i) identity data of said at least one server computer and (ii) identity data of each of said at least one client computer device . . ." (Ex. B at 34:61-63)
Claim 31	"a clearinghouse that stores (i) identity data of said client computer device . . . " (Ex. B at 37:35-36)
Claim 62	"storing (i) identity data of the server computer, (ii) identity data of the client computer device having a hardware key . . ." (Ex. B at 39:55-57)
Claim 87	"storing (i) identity data of the client computer device having a hardware key . . ." (Ex. B at 42:1-2)
Claim 117	"at least one authentication server having an associated database to store (i) identity data of at least one access server . . ." (Ex. B at 45:4-6)
Claim 150	"storing (i) identity data of at least one access server . . ." (Ex. B at 47:26)
Claim 185	"storing (i) identity data of at least one access server . . ." (Ex. B at 50:1)

Thus, it does not make sense to construe only the phrase "identity data of [the] client computer device," when "identity data" has a much broader application in the claims to "server computers" and "access servers" as well.

Second, Defendants improperly attempt to impose a requirement that the "identity data" of the client computer device must include "the digital identification as well as some additional data (e.g., a username and/or a password)." The intrinsic evidence shows that Defendants' proposed construction is wrong. Claim 1 of the '288 patent, for example, recites "said at least one hardware key generating a digital identification, the identity data of said at least one client

computer device comprising said digital identification." (Ex. B at 35:8-10). Claims 31, 62, and 87 contain similar language of the client computer device's "identity data . . . comprising [said/the] digital identification." (*Id.* at 37:42-43, 39:60-62, 42:6-8). "In the patent claim context the term 'comprising' is well understood to mean 'including but not limited to.'" *CIAS, Inc. v. Alliance Gaming Corp.*, 504 F.3d 1356, 1360 (Fed. Cir. 2007). Thus, the claim language "the identity data . . . comprising said digital identification" means that the identity data must include the digital identification, and could include other items as well, but does not necessarily need to. Defendants' proposed construction, on the other hand, violates the commonly understood meaning of "comprising" by requiring that "identity data" include not only the digital identification, but also "some additional data (e.g., a username and/or a password)."

Defendants' proposed construction also violates the principle of claim differentiation. For example, claim 3 of the '288 patent reads: "The system of claim 1, wherein the identity data of said at least one client computer device includes said digital identification and at least one of a username and a password." (Ex. B at 35:39-41). Claim 3 therefore adds the limitation that the identity data must include not only the digital identification, but also "at least one of a username and a password."[10] The addition of this language in claim 3 shows that the client computer "identity data" recited in claim 1 does not, by itself, require anything more than the digital identification. *See Phillips*, 415 F.3d at 1315 ("the presence of a dependent claim that adds a

[10] Similarly, claim 36 reads "The system of claim 31, wherein the identity data of said client computer device includes said digital identification and at least one of a username and a password." (Ex. B at 38:8-10).

particular limitation gives rise to a presumption that the limitation in question is not present in the independent claim.").

Moreover, Defendants' contention that "identity data" must include more than just the "digital identification" is an issue that was previously addressed by the Delaware court. In *VeriSign*, the defendants argued that the term "identity data" "must be the predetermined digital identification along with something else to identify the subscriber client computer." (Ex. K at 19). Accordingly, the defendants proposed that "identity data" should be construed as "information that uniquely identifies the subscriber client computer and which includes the predetermined digital identification from the hardware key as well as additional information not stored on the hardware key." (Ex. G at 21). The Delaware court rejected the defendants' proposed construction, and instead construed "identity data" as simply "data sufficient for the patented system to determine whether a person, organization, and/or computer is authentic and/or is entitled to access said selected protected resources." (Ex. F at 3). This previous construction of "identity data," which is a part of the '288 prosecution history, should be controlling.

Defendants' proposed construction is also improper in its requirement that the "identity data" "uniquely identifies the account holder using the client computer device." As with their proposed construction of "digital identification," Defendants improperly seek to import a description in the specification of "uniquely identif[ying] the account holder" for one preferred embodiment into the claim limitation "identity data." But just as the Delaware court refused to impose a "uniqueness" requirement on the term "digital identification," the court also refused to impose such a requirement on the term "identity data." In *VeriSign*, the defendants proposed that the term "identity data" in the '416 patent claims should be construed as "information that

uniquely identifies the subscriber client computer and which includes the predetermined digital identification from the hardware key as well as additional information not stored on the hardware key." (Ex. G at 21). The Delaware court rejected this argument, holding:

> The term ["identity data"] is not limited, as Defendants have argued, to the identity data that uniquely identifies the subscriber client computer. When discussed in the '416 Patent, the identity data of the subscriber client computer is that identity data which is transmitted by the subscriber client computer and used by the invention to verify the identity of the subscriber. . . . Accordingly, the Court construes "Identity Data" as it relates to the Subscriber Client Computer to mean "data sufficient for the patented system to determine whether a person, organization, and/or computer is authentic and/or is entitled to a[cc]ess said selected computer resources.

(Ex. E at 24). There is no reason for this Court to depart from the Delaware court's prior construction of "identity data."

F. "authenticating"

The term "authenticating" appears in various of the asserted claims of the '288 patent. Prism contends that "authenticating" should be construed consistently, as the Delaware court did in the *Verisign* case. Defendants do not want to construe the term "authenticating" consistently, but instead want to vary its meaning depending on the phrases in which the term "authenticating" appears. The parties' proposed constructions relating to "authenticating" are as follows:

Claim Term	Prism's Proposed Construction	Defendants' Proposed Construction
"authenticating" (independent claims 1, 31, 62, 87, 117, 150, 185-87)	determining that something is, in fact, what it purports to be	Defendants believe that the Court should not construe the word "authenticating" in isolation but rather in the context of the relevant claim language, as set forth [below].

"**authenticating [] the identity of [the/said] client computer device**" (independent claims 1, 31, 62, 87)	No separate construction necessary in light of Prism's proposed construction of "authenticating."	to determine whether the received identity data, including the digital identification, for the account holder matches the identity data for the account holder stored on the clearinghouse
"**to authenticate said digital identification**" (independent claims 117, 187) and "**authenticating … the digital identification**" (independent claims 150, 185, 186)	No separate construction necessary in light of Prism's proposed constructions of "authenticating" and "digital identification."	to determine whether the received digital identification for the account holder matches the digital identification for the account holder stored on the authentication server
"**to authenticate said identity data [of the access server]**" (independent claim 117) and "**authenticating ... the identity data [of the access server]**" (independent claims 150, 185)	No separate construction necessary in light of Prism's proposed constructions of "authenticating" and "identity data."	to determine whether the received identity data for the access server matches the identity data for the access server stored on the authentication server

In *VeriSign*, the parties agreed to the construction of "authenticating" as "determining that something is, in fact, what it purports to be." (Ex. E at 8). The Delaware court approved of this construction. (*Id.*). This construction comports with the ordinary meaning of the term as it is used in the computer industry. (*See* Ex. I, ¶¶ 18-20). For example, "authentication" is defined in The IEEE Standard Dictionary of Electrical and Electronics Terms (6th ed. 1996) as **"**[t]he process of validating a user or process to verify that the user or process is not a counterfeit." (Ex. I, ¶20). Prism asserts that the construction of "authenticating" from the Delaware case should apply to the present action. *See Omega Eng'g*, 334 F.3d at 1334.

Defendants reject the Delaware construction of "authenticating," and instead argue that "authenticating" as used in the '288 claims means matching information regarding "account holders." Defendants once again seek to improperly import the specification's language of identifying "account holders" into the claims, when the claims on their face clearly do not mention anything about "account holders." For the same reasons discussed in Section III.D. above, Defendants' attempt to include the concept of "account holders" as limitations to the asserted claims is improper.

Defendants' proposed constructions are also flawed in that they mistakenly equate "authenticating" with "matching." For example, Defendants propose that the phrase "to authenticate said digital identification" should be construed as "to determine whether the received digital identification for the account holder matches the digital identification for the account holder stored on the authentication server." Setting aside the impropriety of Defendants' references to "the account holder," Defendants' proposed construction is also unduly restrictive in that it requires the system to determine whether the digital identification has perfect correspondence to a digital identification stored in the clearinghouse or authentication server. But this is not the only way in which authentication can occur, and the '288 claims are not restricted to any particular method of authentication. For example, the specification describes a process whereby the digital identification from the hardware key can be encrypted, and the encrypted data is then passed along to be authenticated by the system:

> With respect to the session renewal and referring to FIG. 19, the access device interface reads the digital ID of the access media and submits it to the login interface (block 250), which in turn submits the digital ID to the client cryptographer (block 252). The client cryptographer encrypts the digital ID using the challenge sent by the access device validator and sends the encrypted digital 10 to the access device validator (block 254), which then sends a renew

> session message to the session validator with the encrypted digital ID (block 256). The session validator finds account holder session entry and validates the encrypted digital ID (block 258) and determines whether the validation was successful (block 260). . . . If validation was successful (block 260), the session validator updates the session entry's time of last re-authentication (block 266) and sends a successful session response to the access device validator (block 268).

(Ex. B at 18:46-66). Thus, the specification discloses that authentication of the digital identification does not necessarily require an exact match of the original digital identification from the hardware key with data stored in the system.

Defendants' proposed constructions of the "authenticating" phrases are therefore too narrow and should be rejected.

G. "authorizing"

The term "authorizing" appears in various of the asserted claims of the '288 patent. Prism contends that "authorizing" should be construed according to how the term is commonly understood in the computer industry. Defendants, on the other hand, once again improperly seek to import limiting language regarding "account holders" from the specification into the claims. The parties' proposed constructions relating to "authorizing" are as follows:

Claim Term	Prism's Proposed Construction	Defendants' Proposed Construction
"authorizing" (independent claims 1, 31, 62, 87, 117, 150, 185-87)	determining whether to grant access to	Defendants believe that the Court should not construe the word "authorizing" in isolation but rather in the context of the relevant claim language, as set forth [below].

"**authorizing ... [said/the] client computer device to receive said requested protected resources**" (independent claims 1, 31) and "**authorizing ... the client computer device to receive the protected resources requested by the client computer device**" (independent claims 62, 87)	No separate construction necessary in light of Prism's proposed constructions of "authorizing" and "protected resources."	if the identity data, including the digital identification, for the account holder received from the client computer device matches the identity data stored on the clearinghouse, finding that the account holder has permission to receive the requested protected resources
"**to authorize said at least one client computer device to receive at least a portion of said requested protected computer resources**" (independent claims 117, 187) and "**authorizing [the] client computer device to receive at least a portion of the protected computer resources**" (independent claims 150, 185, 186)	No separate construction necessary in light of Prism's proposed constructions of "authorizing" and "protected computer resources."	if the digital identification received from the client computer device matches the account holder's digital identification stored on the authentication server, determining whether the account holder has permission to receive the requested protected computer resources

Prism's proposed construction of "authorizing" – "determining whether to grant access to" – comports with the ordinary meaning of the term as it is used in the computer industry. (Ex. I, ¶¶ 21-23). For example, the definition of "authorization" in The IEEE Standard Dictionary of Electrical and Electronics Terms (6th ed. 1996) is "[t]he process of verifying that a user or process has permission to use a resource in the manner requested." (Ex. I, ¶ 23). Once "authorizing" is construed, the meaning of the phrases in which this term appears and that Defendants propose construing are readily apparent, and need no further construction. For example, under Prism's proposed construction of "authorizing," the phrase "authorizing ... [said/the] client computer device to receive said requested protected resources" would simply

mean "determining whether to grant the client computer device access to receive said requested protected resources."

Defendants' proposed constructions of the phrases containing the term "authorizing" are improper for the same reasons as their proposed constructions of the "authenticating" phrases. Once again, Defendants seek to improperly import the specification's language of identifying "account holders" into the claims, and requiring that the "digital identification" and "identity data" must exactly match data stored in the system. For the same reasons discussed in Sections III.D.-III.F. above, there is no basis to construe the '288 claims in such a restrictive manner.

H. "clearinghouse"

The parties propose the following constructions for the term "clearinghouse," which appears in asserted independent claims 1, 31, 62, and 87 of the '288 patent:

Claim Term	Prism's Proposed Construction	Defendants' Proposed Construction
"**clearinghouse**" (independent claims 1, 31, 62, 87)	a computer having software capable of storing data and controlling access to protected resources	a computer that, independently of the server computer, authenticates account holders and controls access to protected resources of the server computer

As described in the '288 specification, a "clearinghouse" is a server computer that hosts a database of information regarding users and/or devices and uses that information to control which users and/or devices can access the protected resources of the system. For example, the specification states:

> The transaction clearinghouse is the entity that hosts all of the account and transaction data. The transaction clearinghouse provides a secure interface to the secure transaction servers 34, which enables the secure transaction servers 34 to authenticate the account holders and to send account holders' transaction data to the transaction clearinghouse. The transaction clearinghouse consists of a

> structured query language (SQL) database, which hosts the transaction clearinghouse database as well as an account holder authentication server for authenticating account holders on behalf of the secure transaction servers and processes online applications. The transaction clearinghouse also includes a transaction server that collects transaction data from the secure transaction servers 34 and updates the transaction clearinghouse database.

(Ex. B at 4:24-39).

The claims of the '288 patent shed further light regarding the meaning of "clearinghouse." For example, claim 1 recites that the "clearinghouse" has the following functions:

> . . . at least one ***clearinghouse*** for storing (i) identity data of said at least one server computer and (ii) identity data of each of said at least one client computer device and (iii) authorization data associated with said protected resources;
>
> server software installed on said at least one server computer that forwards the identity data of said at least one server computer and the identity data of each of said at least one client computer device to said at least one ***clearinghouse***;
>
> . . . said at least one ***clearinghouse*** authenticating the identity of said at least one client computer device responsive to a request for said protected resources of said at least one server computer by said at least one client computer device;
>
> said at least one ***clearinghouse*** authenticating the identity of said at least one server computer responsive to said at least one client computer device making the request for said protected resources of said at least one server computer;
>
> said at least one ***clearinghouse*** authorizing said at least one client computer device to receive said requested protected resources, based on said stored authorization data;
>
> and, said at least one ***clearinghouse*** controlling access to said requested protected resources of said at least one server computer responsive to successful authentication of said at least one server computer and of said at least one client computer device making the request and responsive to successful authorization of said at least one client computer device.

(Ex. B at 34:54-35:36). Thus, claim 1 requires that the "clearinghouse" performs the function of 1) storing data regarding the identity of client and server devices in the system; 2) storing data

regarding which devices are authorized to access protected resources; and 3) using the stored data to authenticate client computer devices and authorize them to access protected resources.[11] Consistent with the '288 claims and specification, Prism proposes that "clearinghouse" be construed as "a computer having software capable of storing data and controlling access to protected resources."

Defendants, on the other hand, propose that "clearinghouse" be construed as "a computer that, independently of the server computer, authenticates account holders and controls access to protected resources of the server computer." Defendants' proposed construction is flawed in two respects. First, the proposed language that the clearinghouse "authenticates account holders" directly contradicts both the plain language of the claims as well as the specification. None of the asserted claims contain any language regarding "accounts" or "account holders." Moreover, the claims specifically recite the items that the clearinghouse authenticates, and none of those items are "account holders." For example, as shown above, claim 1 recites that the clearinghouse authenticates "the identity of said at least one client computer device" and "the identity of said at least one server computer." Similarly, claims 31, 62, and 87 also refer to authenticating the identities of client and server computers, as shown below:

Claim 31	"said clearinghouse authenticating the identity of said client computer device . . . " (Ex. B at 37:47-48)
Claim 62	"authenticating, by the clearinghouse, the identity of the client computer device . . ." (Ex. B at 40:4-5)

[11] Claims 31 and 87 do not require the "clearinghouse" to store any identity data of any server devices.

	"authenticating, by the clearinghouse, the identity of the server computer . . ." (Ex. B at 40:8-9)
Claim 87	"authenticating, by the clearinghouse, the identity of the client computer device . . ." (Ex. B at 42:16-17)

As the language of these claims makes clear, the clearinghouse performs the function of authenticating the identity of various physical devices, not "account holders." (*See* Ex. I, ¶¶ 24-26).

Second, Defendants' proposed construction improperly adds the language that the clearinghouse is a computer "independent[] of the server computer." Under the principle of claim differentiation, the term "clearinghouse" cannot be restricted in this way. Claim 6 of the '288 patent depends on claim 1 and recites: "The system of claim 1, wherein said at least one clearinghouse operates as an independent entity and authenticates multiple server computers capable of being at separate physical locations." (Ex. B at 35:49-52). The presence of the additional limitation in claim 6 that the clearinghouse "operates as an independent entity" creates a presumption that this limitation is not a part of claim 1, from which claim 6 depends. *See Phillips*, 415 F.3d at 1315. Prism's proposed construction of "clearinghouse" is therefore the most consistent with the language of the claims and the specification, and should be adopted.

I. "access server"

The parties propose the following constructions for the term "access server," which appears in asserted independent claims 117, 150, and 185-187:

Claim Term	Prism's Proposed Construction	Defendants' Proposed Construction
"**access server**" (independent claims 117, 150, 185-187)	server software that makes available information or other resources	a computer that makes available information or other resources

The parties' only dispute with respect to the construction of "access server" concerns whether the term refers to a software program or a physical computer. Prism's proposed construction – that "access server" refers to software – is supported by the specification and the claims of the '288 patent.

In the field of computer networking, "server" is a commonly used term that can refer to either a computer or a software program, depending upon the particular context in which the term is used. (*See* Ex. I, ¶ 29). The "access server" recited in the '288 claims refer to the "secure transaction server 34" described in the '288 specification. (*See id.* at ¶ 31). As described in one embodiment in the specification, "[the transaction clearinghouse] has a secure interface to communicate with the secure transaction servers 34, which reside on the same machine that hosts the web server." (Ex. B at 4:16-19). This reference to multiple transaction servers residing "on the same machine" indicates that the transactions servers (*i.e.*, the "access servers") are software programs, not hardware. (*See* Ex. I, ¶¶ 30-31).

Indeed, when the inventors of the '288 patent intended for "server" to mean a computer, they made this explicit by using the term "server computer." For example, claims 1, 31, 62, and 87 of the '288 patent refer to a "server computer" providing access to protected resources. By contrast, claims 117, 150, and 185-187 recite an "access server" involved in controlling access to protected resources. The inventors' decision to use the term "access server" rather than "access

server computer" supports the position that "access server" does not refer to a physical computer, but rather software. *See Phillips*, 415 F.3d at 1314 ("Differences among claims can also be a useful guide in understanding the meaning of particular claim terms."). Moreover, under Defendants' proposal, "access server" would have the same construction as "server computer," which would violate the principle that different claim language is presumed to have different scope. *See Forest Labs., Inc. v. Abbott Labs.*, 239 F.3d 1305, 1310 (Fed. Cir. 2001) ("Where claims use different terms, those differences are presumed to reflect a difference in the scope of the claims."). Prism's proposed construction of "access server" is therefore the more reasonable construction, and should be adopted.

J. "authentication server"

The parties propose the following constructions for the term "authentication server" in the asserted claims of the '288 patent:

Claim Term	Prism's Proposed Construction	Defendants' Proposed Construction
"**authentication server**" (independent claims 117, 150, 185-187)	software capable of storing data and permitting access to protected computer resources	a computer that, independently of the access server, authenticates account holders and controls access to protected computer resources of the access server

The parties' proposed constructions differ in several respects. First, Prism's proposed construction is that "authentication server" refers to a software program, whereas Defendant propose that the term refers to a physical computer. Second, similar to their proposed construction of "clearinghouse," Defendants' proposed construction of "authentication server" adds the requirement that the authentication server acts "independently of the access server." Third, Defendants' proposed construction requires that the authentication server "authenticates

account holders." Fourth, Defendants' proposed construction adds the requirement that the protected computer resources are "of the access server." None of these additional requirements proposed by Defendants is proper.

With respect to the first dispute regarding the construction of "authentication server," Prism's position that "authentication server" refers to software rather than a computer is supported by the specification, which states:

> The transaction clearinghouse server is preferably a Sun UNIX server which runs the transaction clearinghouse server processes and the database server. However, the database server could reside on a separate machine…. The transaction clearinghouse consists of a structured query language (SQL) database, ***which hosts the transaction clearinghouse database as well as an account holder authentication server*** for authenticating account holders on behalf of the secure transaction servers and processes online applications.

(Ex. B at 4:21-36). Thus, the specification refers to the clearinghouse (which all parties agree is a computer) as "hosting" an authentication server, which only makes sense if the "authentication server" is a software program, rather than a physical computer. (*See* Ex. I, ¶ 36).

This interpretation is further supported by Figure 3 in the '288 patent. Block 30 in Figure 3 shows the transaction clearinghouse, which is depicted as comprising two software modules – the "authentication server" and the "transaction data server," along with an associated "clearinghouse database." (*See* Ex. B at Fig. 3; 6:26-35). Similarly, block 154 in Figure 16 refers to the step "session initiator sends authenticate (AL) message to clearinghouse's user authentication server," again indicating that the authentication server is software associated with the clearinghouse computer. (*See id.* at Fig. 16; Ex. I, ¶ 36).

Moreover, as discussed in Section III.I. above, when the inventors intended for the claims to cover server computers rather than software, they explicitly used the term "server computer."

Thus, one of skill in the art reading the '288 specification and claims would understand that "authentication server" refers to software, not a computer. (*See* Ex. I, ¶¶ 32-36).

Defendants' proposed construction of "authentication server" should also be rejected because, like their proposed construction of "clearinghouse," Defendants again improperly seek to add the requirement that the authentication server "authenticates account holders" and acts "independently of the access server." For similar reasons discussed above, Defendants' proposed construction should be rejected. Claims 117, 150, and 185-187, in which the "authentication server" term appears, specifically state that the function of the authentication server is to authenticate "identity data" and "digital identification" of devices, not account holders. Specifically, these claims state:

Claim 117	"said at least one authentication server adapted to ***authenticate said identity data*** [of at least one access server] ***and said digital identification*** [associated with at least one client computer device] responsive to a request for said protected computer resources by said at least once client computer device . . ." (Ex. B at 45:21-24) (emphasis added)
Claim 150	"***authenticating***, by the at least one authentication server, ***the identity data*** [of at least one access server] ***and the digital identification*** [associated with at least one client computer device] forwarded by the at least one access server . . ." (Ex. B at 47:42-44) (emphasis added)
Claim 185	"***authenticating***, by the at least one authentication server, ***the identity data*** [of at least one access server] ***and the digital identification*** forwarded by the at least one access server . . ." (Ex. B at 50:18-20) (emphasis added)
Claim 186	"***authenticating***, by the at least one authentication server, ***the digital identification*** [associated with at least one client computer device] forwarded by the at least one access server . . ." (Ex. B at 50:54-56) (emphasis added)
Claim 187	"said at least one authentication server adapted to ***authenticate said digital identification*** [associated with at least one client computer device] responsive to a request for said protected computer resources by said at least once client computer device . . ." (Ex. B at 52:1-4) (emphasis added)

As shown above, claims 117, 150, and 185 state that the authentication server authenticates two pieces of information: 1) identity data of an access server; and 2) a digital identification associated with a client computer device. Claims 186 and 187 state only that the authentication server authenticates a digital identification associated with a client computer device. In each of these claims, however, there is no mention of authenticating "account holders," but rather specific data relating to server and client devices. Thus, Defendants' proposed construction of "authentication server" should be rejected, as it would directly contradict the plain language of the claims. (*See* Ex. I, ¶¶ 37-38).

In addition, Defendants' proposed construction improperly attempts to limit "authentication server" to controlling access to protected computer resources "of the access server." To the extent Defendants are proposing that the protected computer resources must be physically stored on the access server, there is nothing in the language of the claims that requires such a reading of "authentication server." (*See* Section III.C. above). Instead, claims 117, 150, and 185-187 merely recite "protected computer resources provided via an Internet Protocol network," with no restriction as to where those protected resources may be located. (*See, e.g.*, Ex. B at 45:1-2).

K. "selectively requiring . . . [said/the] client computer device to forward"

The parties propose the following constructions for the term "selectively requiring . . . [said/the] client computer device to forward" in the asserted claims of the '288 patent:

Claim Term	Prism's Proposed Construction	Defendants' Proposed Construction
"**selectively requiring ... [said/the] client computer device to forward**" (independent claims 1, 31, 62, 87)	Choosing to require that the client computer device transmit certain information	during an operating session, periodically requiring the client computer device to forward

This phrase appears in the following contexts in claims 1, 31, 62, and 87:

Claim 1	"said server software installed on said at least one server computer selectively requiring said at least one client computer device to forward said digital identification to said at least one server computer . . ." (Ex. B at 35:12-15)
Claim 31	"said server computer selectively requiring said client computer device to forward said digital identification to said server computer; . . . " (Ex. B at 37:44-46)
Claim 62	"selectively requiring the client computer device to forward its identity data to the server computer . . ." (Ex. B at 39:63-64)
Claim 87	"selectively requiring the client computer device to forward its identity data to the server computer; . . ." (Ex. B at 42:9-10)

Prism's proposed construction clarifies that "selectively requiring" means "choosing to require," and also clarifies that the action "to forward" means to "transmit" certain information. This is consistent with the Delaware court's claim construction order, in which the court accepted the parties' agreement in that case that "requiring . . . to forward" means "requiring that certain information be transmitted." (Ex. E at 8).

Prism's proposed construction is also consistent with the language of the claims, which as shown above refer to forwarding "digital identification" and "identity data" from one computing device to another. "To forward" in this context therefore means to transmit information from one location to another.

In addition, Prism's proposed construction of "selectively requiring" to mean "choosing to require" comports with the dictionary definition of "select," which is "to choose (as by fitness or excellence) from a number or group : pick out . . . to make a choice." (Ex. L, Merriam-Webster's Collegiate Dictionary, 10th ed. (1999)).

Defendants propose that "selectively requiring" should mean "during an operating session, periodically requiring." This construction improperly imposes a temporal requirement (that the action of "requiring" must occur "during an operating session") as well as a frequency requirement (that the action of "requiring" must occur "periodically" as opposed to just one time). Such a construction is not supported by the intrinsic evidence.

First, there is nothing in the language of the claims that requires the forwarding of the digital identification or identity data to occur during any particular time frame, much less during an "operating session." Indeed, it is not even clear what Defendants mean by an "operating session." This term is not defined anywhere in the specification. And while the Delaware court did construe "operating session" as the term appears in the '416 claims to mean "a period of communication between the subscriber client computer and the first server computer that follows successful initial authentication and ends upon termination of authorized access, such as upon a log-out or time-out due to prolonged activity" (Ex. F at 2), Defendants have not indicated whether the Delaware construction was their intended meaning for "operating session." Thus, Defendants' proposed language "during an operating session" is both unsupported and needlessly confusing.

Second, Defendants' proposal that the action of "selectively requiring" means "periodically requiring" is improper under the principle of claim differentiation. Claim 9 of the '288 patent, which depends on claim 1, reads: "The system of claim 1, wherein said at least one server computer ***intermittently requires*** said at least one client computer device to forward said digital identification to said at least one server computer." (Ex. B at 35:61-64) (emphasis added). Since dependent claim 9 adds the limitation of "intermittently" (*i.e.*, "periodically")

requiring the client computer device to forward the digital identification, this limitation cannot be present in claim 1. *See Phillips*, 415 F.3d at 1315 ("the presence of a dependent claim that adds a particular limitation gives rise to a presumption that the limitation in question is not present in the independent claim").

Defendants' proposed construction is also flawed in that Defendants do not offer any clarification as to the meaning of the term "to forward." Prism's construction addresses this term by clarifying that "forward" means "transmit," a construction that is consistent with the Delaware court's constructions. (Ex. F at 6-7).

L. "adapted to forward"

The parties propose the following constructions for the phrase "adapted to forward" in the asserted claims of the '288 patent:

Claim Term	Prism's Proposed Construction	Defendants' Proposed Construction
"adapted to forward" (independent claims 117, 187)	capable of transmitting	configured to forward

In *VeriSign*, the parties agreed that the term "adapted to forward" in the '416 claims should be construed as "capable of transmitting," and the Delaware court adopted this construction. (Ex. E at 8). As with the other terms construed in Delaware, the Delaware court's construction of "adapted to forward" was made part of the '288 prosecution history. Prism proposes that this Court adopt the Delaware court's construction of "adapted to forward," as there is no significant difference in how this term is used in the '288 claims as compared to the '416 claims.

Defendants reject the Delaware construction of "adapted to forward," and instead propose construing the term to mean "configured to forward." But this simply replaces the word "adapted" with "configured," which does little to clarify what it means for a server to be "adapted to forward" data to another server, as recited in the claims. The Delaware construction provides this clarification and is consistent with the language of the '288 claims, and there is no reason to depart from it here.

M. "Internet Protocol network"

The parties propose the following constructions for the term "Internet Protocol network" in the asserted claims of the '288 patent:

Claim Term	Prism's Proposed Construction	Defendants' Proposed Construction
"Internet Protocol network" (independent claims 117, 150, 185-187)	a network using any protocol of the Internet Protocol Suite including at least one of IP, TCP/IP, UDP/IP, and HTTP	an untrusted network that uses a protocol of the Internet Protocol Suite including at least one of IP, TCP/IP, UDP/IP, and HTTP

The only significant difference between the parties' competing constructions is that Defendants contend that an "Internet Protocol network" must be an "untrusted" network, whereas Prism contends that the phrase "Internet Protocol network" is not so limited. As discussed in Section III.B. above, the parties agree than an "untrusted network" means "a public network with no controlling organization, with the path to access the network being undefined and the user being anonymous." An "Internet Protocol network," however, is not limited to a public network. For example, organizations can set up private networks that are not accessible to the general public, yet utilize one or more protocols of the Internet Protocol Suite for

communications within that network. (*See* Ex. I, ¶ 44). Such private networks would be considered "trusted," rather than "untrusted," Internet Protocol networks. (*See id.* at ¶ 45).

In fact, the '288 specification discloses a specific example of a private, and therefore "trusted," Internet Protocol network:

> The account holders are connected to the Internet 38 via a modem connection or via a similar means, and the Internet 38 has a connection to the server. The server 34 is connected to a local area network (LAN) 40 through a firewall computer 42. A firewall is used to separate a local area network from the outside world. In general, a local area network is connected to the outside world by a "gateway" computer. This gateway machine can be converted into a firewall by installing special software that does not let unauthorized TCP/IP packets passed from inside to outside and vice versa.

(Ex. B at 3:59 – 4:2). This passage describes a private network (a local area network separated from public access by a firewall computer) within which communications are passed using TCP/IP, a protocol that the parties agree is a part of the Internet Protocol Suite. (*See* Ex. I, ¶ 45). Thus, the specification clearly contemplates that there can be "Internet Protocol networks" that are not "untrusted networks."

Furthermore, the language of the claims shows that the inventors of the '288 patent specifically used the term "Internet Protocol network" to mean something other than an "untrusted network." For example, the table below shows a comparison between the preambles of claims 31 and 117 in the '288 patent:

Claim 31	Claim 117
"A system for protecting resources of a server computer, said server computer providing said protected resources to a client computer device **via an untrusted network**, without necessarily protecting other computer resources provided by said server computer and by other server computers to	"A system for controlling access to protected computer resources provided **via an Internet Protocol network**, the system comprising: . . ." (Ex. B at 45:1-3) (emphasis added)

other client computer devices, comprising: . . ." (Ex. B at 37:28-34) (emphasis added)	

The fact that the inventors of the '288 patent chose to use the term "untrusted network" in some claims and "Internet Protocol network" in others demonstrates that these terms to have different meanings. *See Comark Commc'ns, Inc. v. Harris Corp.*, 156 F.3d 1182, 1187 (Fed. Cir. 1998) ("There is presumed to be a difference in meaning and scope when different words or phrases are used in separate claims.") (quoting *Tandon Corp. v. United States Int'l Trade Comm'n*, 831 F.2d 1017, 1023 (Fed. Cir. 1987).

III. CONCLUSION

For the reasons set forth above, Prism respectfully requests that the Court construe all of the disputed terms of the '288 patent claims in accordance with Prism's proposed constructions.

Dated: October 17, 2011

Respectfully submitted,

/s/ Christopher D. Banys
Christopher D. Banys

THE LANIER LAW FIRM, P.C.
Christopher D. Banys SBN: 230038 (California)
Carmen M. Aviles SBN: 251993 (California)
Daniel M. Shafer SBN: 244839 (California)
Richard C. Lin SBN: 209233 (California)
2200 Geng Road, Suite 200
Palo Alto, CA 94303
Tel: (650) 322-9100
Fax: (650) 322-9103
cdb@lanierlawfirm.com
cma@lanierlawfirm.com

dms@lanierlawfirm.com
rcl@lanierlawfirm.com

THE LANIER LAW FIRM, P.C.
W. Mark Lanier SBN: 11934600 (Texas)
(Admitted Pro Hac Vice)
Dara G. Hegar SBN: 24007280 (Texas)
(Admitted Pro Hac Vice)
6810 FM 1960 West
Houston, TX 77069
Tel: (713) 659-5200
Fax: (713) 659-2204
wml@lanierlawfirm.com
dgh@lanierlawfirm.com

PRISM TECHNOLOGIES, LLC
André J. Bahou – V.P. and Chief Intellectual Property Officer SBN: 483516 (D.C.)
878 Arlington Heights Dr., Suite 400
Brentwood, TN 37027
Tel: (615) 712-6580
Fax: (402) 578-1447
aj.bahou@prsmip.com

Local Counsel:

KOLEY JESSEN P.C., L.L.O.
Michael C. Cox SBN: 17588
Daniel J. Fischer SBN: 22272
1125 S. 103rd St., Suite 800
Omaha, NE 68124
Tel: (402) 390-9500
Fax: (402) 390-9005
Mike.Cox@koleyjessen.com
Dan.Fischer@koleyjessen.com

ATTORNEYS FOR PLAINTIFF
PRISM TECHNOLOGIES, LLC

CERTIFICATE OF SERVICE

I hereby certify that all counsel of record who are deemed to have consented to electronic service are being served with a copy of this document via the Court's CM/ECF system on this 17th day of October 2011.

/s/ Vicki Comer
Vicki Comer